TEOREMA DELL'ELEMENTO PRIMITIVO

Teorema: $\mathbb{F}$ campo.

$G \subseteq \mathbb{F}^*$ sottogruppo finito $\Rightarrow$ G è ciclico.

Dim.

Sia $S := \{ \mathrm{ord}(g) \mid g \in G \} \subseteq \mathbb{N}$ Possibili ordini degli elementi di G.

Sia $m := \max S$. Devo provare che $m = |G|$.

Nota che $S = \{$divisori di $|G|\}$ e quindi che

$\boxed{m \leq |G|}$ (dunque basta provare che $m \geq |G|$).

Studio le proprietà aritmetiche dell'insieme S.

CLAIM 1: $a, b \in S$, $\gcd(a,b) = 1 \Rightarrow a \cdot b \in S$.

Dim:

$a, b \in S \Rightarrow \exists\, \alpha, \beta \in G$ tali che $\mathrm{ord}(\alpha) = a$, $\mathrm{ord}(\beta) = b$.

Dico che $ab = \mathrm{ord}(\alpha\beta) \in S$. Osservo per cominciare che:

$$(\alpha\beta)^{ab} = (\alpha^a)^b \cdot (\beta^b)^a = 1^b \cdot 1^a = 1 \Rightarrow \boxed{c = \mathrm{ord}(\alpha\beta) \text{ divide } ab}$$

(G è commutativo; Lagrange.)

Adesso

$$1 = (\alpha\beta)^{c\cdot a} = \alpha^{ca}\cdot\beta^{c\cdot a} = \beta^{ca} \Rightarrow b \mid c\cdot a$$

($c = \mathrm{ord}(\alpha\beta)$; $a = \mathrm{ord}(\alpha)$; ↑ Lagrange)

$$\Rightarrow \boxed{b \mid c}$$

($\gcd(a,b)=1$)

Con un calcolo analogo (quale?) si trova che $\boxed{a \mid c}$.

$$a \mid c,\ b \mid c,\ \gcd(a,b)=1 \Rightarrow ab \mid c \Rightarrow c = ab.$$

(↑ $c \mid ab$)

CLAIM 2: $a\cdot b \in S \Rightarrow a, b \in S$

Dim:

$$a\cdot b \in S \Rightarrow \exists\, x \in G \text{ t.c. } \mathrm{ord}(x) = a\cdot b$$

Dico che $\beta := \alpha^a$ ha ord $= b$. Infatti:

$$\beta^b = (\alpha^a)^b = \alpha^{a\cdot b} = 1 \Rightarrow \boxed{s = \mathrm{ord}(\beta) \text{ divide } b}$$

(↑ Lagrange)

D'altra parte

$$1 = \beta^s = (\alpha^a)^s = \alpha^{a\cdot s} \Rightarrow ab \mid as \Rightarrow \boxed{b \mid s}$$

($s = \mathrm{ord}(\beta)$; ↑ ancora Lagrange!)

Dunque $b = s = \mathrm{ord}(\beta)$. Analogamente si mostra che

$\gamma = \beta^b$ ha ordine $= a$.

CLAIM 3: $\quad a, b \in S \Rightarrow \operatorname{mcm}(a,b) \in S$.

Dim.

$$\left.\begin{aligned} a &= \gcd(a,b) \cdot s \\ b &= \gcd(a,b) \cdot s' \end{aligned}\right\} \Rightarrow \quad a, b, \gcd \in S$$

↑ PASSO 2

$$\operatorname{mcm} = s \cdot s' \cdot \gcd \in S$$

↑ PASSO 1.

CLAIM 4: $\quad \alpha^m = 1$ per ogni $\alpha \in G$.

Prendo $\alpha \in G$, $\operatorname{ord}(\alpha) = a$ e osservo che:

$$m \leq \operatorname{mcm}(a,m) \leq m \Rightarrow \boxed{\operatorname{mcm}(a,m) = m}$$

↑ mcm ∈ S e $m = \max S$

Dunque:

$$\alpha^m = \alpha^{\operatorname{mcm}(a,m)} = \alpha^{k \cdot a} = (\alpha^a)^k = 1^k = 1.$$

↑ $\operatorname{mcm}(a,m) = k \cdot a$

PASSO 5: $m \geq |G|$.

Ogni elemento di G soddisfa l'equazione

$$z^m - 1 = 0$$

che ha al più m soluzioni in $\mathbb{F}$, dunque necessariamente $|G| \leq m$.

QED.

Per esempio

→ $(\mathbb{Z}/p\mathbb{Z})^*$ con p primo è ciclico essendo il gruppo moltiplicativo del campo $\mathbb{Z}/p\mathbb{Z}$.

→ $\mathbb{F}$ campo finito $\Rightarrow \mathbb{F}^*$ è ciclico.

→ Il gruppo delle radici dell'unità

$$C_n = \{ z \in \mathbb{C}^* \mid z^n - 1 = 0 \}$$ è ciclico.